2024

Installer et configurer un Firewall Pfsense



BRIEUC LE_FAUCHEUR Saint-Sauveur 02/10/2024 **Objectif :** Installer et Configurer un Firewall PFSENSE dans une infrastructure virtuelle.

Un schéma est présenté au tableau à l'ensemble des étudiants avec des explications.

Adressage de l'infrastructure :

- Passerelle : 192.168.0.253
- Adresse IP WAN du Firewall : adresse à mettre par les étudiants (ils doivent se concerter)
- Adresse IP LAN : 172.16.1.253 (/16)
- Adresse IP du poste derrière le FIRÉWALL : 172.16.1.1 (/16)

Etapes de réalisation et tests :

- 1 Installer et configurer le Firewall PFSENSE (IP WAN/ IP LAN)
- 2 Vérification de l'accès au Firewall par l'interface de gestion (navigateur)

3 - Vérifier l'accès à internet sur l'adresse IP LAN (le poste derrière le Firewall doit avoir accès à internet)

4 - Test de blocage du site internet ECOLE DIRECTE (par exemple) - Etude du fonctionnement du filtrage URL

1 - Installer et configurer le Firewall PFSENSE (IP WAN/ IP LAN)

Pour commencer on va installer notre Pare-feu Pfsense sous virtual box.

 Crée une machine vir 	tuelle			
Nom et système o	l'exploitation			
Veuillez choisir un nom e de système d'exploitatio repris au travers de Virtu	un dossier pour la no n que vous envisagez JalBox pour identifier	ouvelle machine vii z d'y installer. Le n cette machine.	tuelle et sélectior om que vous chois	iner le type sirez sera
Nom :	Pfsense_AP			
Dossier de la machine :	D:\VirtualBox\AP	-KALI		~
Type :	BSD			- 64
Version :	FreeBSD (64-bit)			·
			a :	
		Mode expert	Suivant >	Annuler

On fait suivant jusqu'à la lancer, mais avant de la lancer on va bien configurer le réseau de la machine de sorte à ce que l'« adaptateur 1 » sois en **Accès par pont** et l'«adaptateur 2» en Réseau interne.

On lance, sa demande au démarrage sur quoi booter, on met notre iso pfsense



On procède a l'installation

Pfsense_AP [En fonction] - Oracle VM VirtualBox	- 🗆 ×
Fichier Machine Écran Entrée Périphériques Aid	2
La machine virtuelle signale que le système d'exploitation invité ne	e supporte pas l'intégration de la souris pour le mode vidéo actuel. 🙁 🚫
Configure Options:	figuration
<pre>>> Install T root type/Disks:</pre>	Proceed with Installation stripe: 1 disk * pfSense YES NO GPT (BIOS) 1g NO NO
(Select)	<cancel></cancel>
Create ZFS boot pool with displayed	options

on fais select et après Yes

Normalement on arrive ensuite a cette endroit, cette étape est cruciale, il faut dans la barre virtual box aller dans **Périphériques** -->**Lecteur Optique** --> **Éjecter le lecteur de disque existant**

pfSense Installer	
	The installation is now finished. Before exiting the installer, would you like to open a shell in the new system to make any final manual modifications?
	< Yes > < <mark>`</mark> 1 <mark>□ ></mark>

On éteind la machine et on la redémarre

On est maintenant sur l'interface on vas maintenant configurer le WAN et le LAN,

On commence par le WAN, on met notre ip	192.168.0.196 en /24, et on met la passerelle
Pour le LAN on se met en 172.16.1.253 en ,	/16.
JirtualBox Virtual Machine - Netgate	Device ID: 1e3652a09e62d81048a2
*** Welcome to pfSense 2.6.0-RELEASE	(amd64) on pfSense ***
	192.168.0.196/24
LAN (lan) \rightarrow em1 \rightarrow v4	: 172.16.1.253/16
0) Logout (SSH only)	9) pfTop
1) Assign Interfaces	10) Filter Logs
2) Set interface(s) IP address	11) Restart webConfigurator
 Reset webConfigurator password 	12) PHP shell + pfSense tools
4) Reset to factory defaults	13) Update from console
5) Reboot system	14) Enable Secure Shell (sshd)
6) Halt system	15) Restore recent configuration
7) Ping host	16) Restart PHP-FPM
8) Shell	
inter an option:	

On peut maintenant aller sur notre Windows7 Test pour rentrer notre réseau (réseau interne)

Proprietes de : Protocole Internet versi	ion 4 (TCP/IPv4)
Général	
Les paramètres IP peuvent être déter réseau le permet. Sinon, vous devez c appropriés à votre administrateur rése	minés automatiquement si votre Jemander les paramètres IP eau.
Obtenir une adresse IP automation	quement
• Utiliser l'adresse IP suivante :	
Adresse IP :	172.16.1.1
Masque de sous-réseau :	255.255.0.0
Passerelle par défaut :	172 . 16 . 1 . 253
 Obtenir les adresses des serveur 	s DNS automatiquement
O Utiliser l'adresse de serveur DNS	suivante :
Serveur DNS préféré :	1.1.1.1
Serveur DNS auxiliaire :	• • •
🔲 Valider les paramètres en quitta	nt Avancé
	OK Annuler

On peut test en ping 8.8.8.8, si ça ping tout est bon. On installe Firefox (car Google n'a plus de *32)

Et on peut accéder à notre interface de configuration web. Les logs par défaut son admin pfsense

On change tout de suite le mot de passe par défaut en HOS4mdp

2- Bloquer le site Ecoledirecte.com

On vas maintenant passer a l'étape du bloquage

En premier lieux, on vas créer un alias, correspondant au site que l'on veut, par exemple en nom on vas mettre ici ecoledirecte, et la valeur sera <u>www.ecoledirecte.com</u>

Firewall / A	Aliases / IP		Lat. 🚱
IP Ports URL	s All		
Firewall Alias	es IP		
Name	Values	Description	Actions
ecoledirecte	www.ecoledirecte.com	ecoledirecte	e 🗇 🗇 💼
			+ Add 1 Import

Par la suite, on vas dans services : DNS Forwader, on coche enable DNS Forwarder et on vas ajouter des hosts comme l'image ci-dessous :

Host Overri	des			
Host	Domain	IP	Description	Actions
ecoledirecte	com	152.228.241.34		*
www	ecoledirecte.com	152.228.241.34		* 🛅
				🕂 Add

Et on vas maintenant créer la règle dans Firewall / Rules / LAN

	Block				~
	Choose what to Hint: the differe port unreachab silently. In eithe	o do with packets that m ence between block and le for UDP) is returned to r case, the original pack	atch the criteria sp reject is that with r o the sender, where set is discarded.	pecified below. reject, a packet (TCP I eas with block the pac	RST or ICMP oket is dropped
Disabled	Disable this	rule			
	Set this option	to disable this rule with	out removing it from	m the list.	
Interface	LAN				~
	Choose the inte	erface from which packe	ets must come to n	natch this rule.	
Address	[10] 4				
Address	IPv4				~
			N		
Protocol	Any		15		~
	Choose which I	P protocol this rule sho	uld match.		
	Choose which I	P protocol this rule sho	uld match.		
ource	Choose which I	P protocol this rule sho	uld match.	Course Address	
ource <u>Source</u>	Choose which I	P protocol this rule sho	uld match.	Source Address	1 ~
ource <u>Source</u>	Choose which I	P protocol this rule sho	uld match.	Source Address	/ ~
ource <u>Source</u> estination	Choose which I	P protocol this rule sho	uld match.	Source Address	/ ~
ource <u>Source</u> estination Destination	Choose which I Invert match	P protocol this rule sho any Single host or alia	uld match.	Source Address	/ v
ource <u>Source</u> estination <u>Destination</u>	Choose which I Invert match Invert match	P protocol this rule sho any Single host or alia	uld match.	Source Address ecoledirecte	/ v
ource <u>Source</u> estination Destination	Choose which I Invert match Invert match	P protocol this rule sho any Single host or alia	uld match.	Source Address ecoledirecte	/ v
ource <u>Source</u> estination Destination ctra Option Log	Choose which I Choose which I Invert match Is Log packets	P protocol this rule sho any Single host or alia	uld match.	Source Address ecoledirecte	/ v
ource Source estination Destination ctra Option Log	Choose which I Choose which I Invert match Is Log packets Hint: the firewa of logging, com page).	P protocol this rule sho any Single host or alia that are handled by thi Il has limited local log s sider using a remote sys	s rule pace. Don't turn or slog server (see the	Source Address ecoledirecte	/ v / v
Source Source estination Destination ctra Option Log	Choose which I Choose which I Invert match Log packets Hint: the firewa of logging, coni page). Blocage site E	P protocol this rule sho any Single host or alia that are handled by thi Il has limited local log s sider using a remote sys coleDirecte	s rule pace. Don't turn or slog server (see the	Source Address ecoledirecte	/ v

← → C
 ♦ https://www.ecoledirecte.com
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦
 ♦

Temps de connexion dépassé

On vas maitenant désactiver la règle pour la suite du TP, on vas maintenant installer et configurer Squid Proxy server

Pour se faire on va d'abord mettre à jour notre Pfsense avec la commande « 13 » jusqu'à arriver à la 7.2